APCS/DGPAd

Delitos praticados por meios eletrônicos

Perguntas e respostas

1. Clonagem de WhatsApp

O golpe ocorre da seguinte forma:

O criminoso liga ou envia uma mensagem se passando por um funcionário de site de compra ou de um banco e diz que estará encaminhando um código promocional ou código de confirmação. Ele pede para que a vítima informe esse código que, na verdade, é a verificação do WhatsApp e com ele o criminoso consegue clonar a conta do consumidor.

Após a clonagem, o criminoso passa a enviar mensagens para os contatos da vítima, se passando por ela, pedindo dinheiro. As desculpas para solicitar dinheiro emprestado são as mais diversas, e na maioria das vezes os alvos principais da investida são os parentes mais próximos e amigos que, acreditando na mensagem, acabam depositando ou transferindo valores seguindo as coordenadas do criminoso.

Como evitar o golpe:

a) Ative a "Confirmação em duas etapas" no WhatsApp. Acesse o link e veja como: https://faq.whatsapp.com/general/verification/about-two-step-verification/?lang=pt_br
b) NUNCA forneça o código verificador que você recebe via SMS em seu celular.
c) Não instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém pelo whatsapp.
d) Desconfie de situações em que a pessoa solicita a realização de transferências e pagamentos em caráter de urgência.
e) Ligue para a pessoa que solicitou o dinheiro e verifique se realmente é ela quem está solicitando a transação.

Caso tenha sido vítima, o que fazer:

Vítima do celular clonado
a) Envie um e-mail para support@whatsapp.com com o assunto "CONTA HACKEADA – DESATIVAÇÃO DE CONTA". Relate o ocorrido e siga as instruções do provedor.
b) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**
c) Peça para amigos e familiares excluírem o telefone clonado de grupos e alertarem o máximo de contatos em comum sobre o ocorrido.

Vítima foi quem fez o pagamento
a) Entre em contato com o banco e tente bloquear o valor.
b) Providencie cópia (prints) das conversas realizadas, bem como do comprovante de pagamento.
c) Em posse dessas informações, procure uma Delegacia de Polícia para o registro de Boletim de Ocorrência.

2. Boleto Falso

O golpe ocorre da seguinte forma:

O boleto de cobrança é um instrumento de pagamento pelo qual o emissor, denominado “Beneficiário”, receberá em sua conta o valor referente a um produto ou serviço.

O criminoso, valendo-se de engenharia social ou de um link fraudulento, **altera o código de barras** de modo que o valor caia na conta do integrante da quadrilha.

Como evitar o golpe:

a) Verifique se os dados do “Beneficiário” correspondem aos de quem lhe vendeu o produto ou serviço.
b) Confira se os três primeiros números do código de barras correspondem ao banco cuja logomarca aparece no boleto.
c) Desconfie se o código de barras estiver com falhas que apresentem espaços excessivos entre as barras ou qualquer outra alteração que impossibilite o reconhecimento pela leitora.
d) Sempre que tiver dúvidas sobre a veracidade de um boleto de cobrança, consulte diretamente o fornecedor que o emitiu.
e) Evite reimprimir boletos de cobrança em sites que não sejam do banco emissor do boleto. Evite negociar valores de descontos de boletos com pessoas estranhas, ou que se identificam como funcionários dos bancos ou de empresas de cobrança.

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

3. Fraudes bancárias

Alguns tipos de fraudes bancárias mais recorrentes:

Falso funcionário ou falsa central de atendimento: O estelionatário finge ser funcionário da instituição financeira e diz estar com problemas no cadastro ou irregularidades na conta. A vítima fornece informações sobre sua conta, e com isso o bandido realiza transações fraudulentas.

Falso motoboy: Integrantes da quadrilha ligam para a vítima e dizem pertencerem à central de relacionamento do banco. Afirmam que houve problemas com o cartão da vítima e pedem que ela digite sua senha numérica no teclado do telefone. Na sequência, dizem que enviaram um motoboy na casa da vítima para pegar o cartão. Em posse do cartão e a senha, realizam operações espúrias.

Phishing: O criminoso envia links, e-mails e SMS para a vítima com mensagens que, na maioria das vezes, exploram as emoções (curiosidade, oportunidade única, medo, etc), fazendo com que ela clique nos links e anexos que subtraem dados pessoais ou induzem a realizar cadastros ou fornecer informações.

Como evitar o golpe:

a) Evite usar computadores públicos e redes abertas de wi-fi para acessar conta bancária ou fazer compras online.
b) NUNCA abra e-mails de origem ou de procedência duvidosa.
c) Não execute programas, abra arquivos ou clique em links que estejam anexados ou no corpo desses e-mails.
d) Delete esses e-mails e, caso tenha clicado em alguma parte deste e-mail e executado um programa, comunique imediatamente ao seu banco o ocorrido e altere todas as suas senhas de acesso à sua conta bancária em outro computador confiável, ou no mesmo, após uma verificação completa de infecção de vírus por um técnico confiável;
e) NUNCA utilize seu cartão para fazer compras em sites desconhecidos.

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**

4. Sites de comércio eletrônico fraudulentos

Prática criminosa que tem como alvo clientes de sites de comércio eletrônico.

O golpe ocorre da seguinte forma:

Nessa modalidade, o golpista cria uma página na internet muito semelhante à verdadeira, levando a vítima a acreditar que está efetuando uma compra legítima. Após selecionar os produtos e efetuar o pagamento, a vítima não recebe a mercadoria, quando então percebe que “caiu em um golpe”.

Para aumentar as chances de sucesso, o estelionatário utiliza artifícios, tais como: envio de spams, oferta de produtos com valor abaixo do valor de mercado, propagandas através de links patrocinados, dentre outros.

Além do comprador, as empresas que tiveram seus nomes utilizados indevidamente, ou ainda, as pessoas que tiveram seus dados utilizados para criação do site ou para a abertura de “empresas fantasmas”, também são vítimas.

Como evitar o golpe:

Algumas dicas são indispensáveis, para que possamos ter a certeza que estamos fazendo uma compra legítima, com segurança:

a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;
b) Leia atentamente as informações dos sites e do produto que deseja comprar. Normalmente, sites fraudulentos podem conter erros de português ou ainda sobre as informações técnicas do produto. Verifique também se há CNJP cadastrado na página ou canais de comunicação;
c) Faça uma pesquisa de mercado do valor do produto que deseja adquirir. Desconfie de preços muito baixos;
d) Realize pesquisas na internet para obter informações a respeito da reputação do site em que deseja efetuar compras. Essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon (https://www.procon.sp.gov.br/).
e) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;
f) Evite clicar em links que direcionam a navegação diretamente ao site de compras. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador. **Atenção:** os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro. Exemplo: www.americanas.com.br (site verdadeiro) e www.lojasamercanas.com.br (site falso – exemplo fictício). Note que no exemplo do site falso foi incluído o nome “lojas” e a letra “i” do nome “americanas” foi suprimida.

Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);
b) Faça um print da página e do produto anunciado;
c) Providencie uma cópia do boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou rregistre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

5. Golpe do falso leilão ou falso empréstimo

O golpe ocorre da seguinte forma:

O Golpe do Falso Leilão trata-se de crime praticado pela internet, no qual o estelionatário cria um site falso, contendo fotografias de veículo para simular um leilão online. Após efetuar o lance, a vítima recebe a informação de que venceu o leilão e recebe um termo de arrematação, contendo instruções para a retirada do veículo e pagamento. Após transferir o valor para a conta indicada no termo de arrematação, a vítima não consegue mais nenhuma forma de contato com a empresa que realizava o leilão, quando percebe que caiu em um “golpe”.

Os falsos sites de leilão podem possuir informações de Leiloeiro que já atua no mercado, sem que ele tenha conhecimento de que seus dados estejam sendo utilizados indevidamente. As informações contidas nos sites falsos e os procedimentos adotados pela empresa durante o leilão induzem a vítima a acreditar que está realizando uma transação legítima. Assim como nos casos dos falsos sites de comércio eletrônicos, os preços baixos dos veículos leiloados atraem as vítimas.

Como evitar o golpe:

Algumas dicas são indispensáveis para que possamos ter a certeza que estamos fazendo uma compra legítima, com segurança:

a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;
b) Leia atentamente as informações contidas no site e do veículo que deseja arrematar. Normalmente sites fraudulentos podem conter erros de português e erros nas especificações técnicas do veículo leiloado.
c) Pesquise o CNPJ e do endereço informados junto ao site;
d) Desconfie de preços muito baixos e faça uma pesquisa em relação ao veículo que deseja arrematar;
e) Realize pesquisas na internet para obter informações a respeito da reputação do site. Essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon (https://www.procon.sp.gov.br/);
f) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;
g) Confira para quem o pagamento está sendo realizado. No termo de arrematação, a conta bancária informada para a transferência deve estar em nome do Leiloeiro. Não efetue o pagamento, caso haja qualquer divergência;
h) Evite clicar em links que direcionam a navegação diretamente ao site de leilão online. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador.

Atenção: os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro, sendo modificado de forma quase imperceptível, portanto, verifique atentamente o endereço a fim de se certificar se o site em que está se conectando é o site verdadeiro.

Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);
b) Faça um print da página e do produto anunciado;
c) Providencie uma cópia do termo de arrematação, boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

Importante: Realize contato com a instituição bancária utilizada para efetuar o pagamento, para verificar a possibilidade de bloquear o valor na conta beneficiada.

6. Crimes contra a honra

O golpe ocorre da seguinte forma:

Infelizmente as redes sociais têm sido utilizadas por criminosos para ofender a honra de outrem ou até mesmo para cometer ameaças a integridade física de pessoas de bem. A honra, na concepção comum, pode ser entendida como um conjunto de atributos morais, intelectuais e físicos de uma pessoa.

O Direito Penal protege o bem jurídico da honra objetiva, por meio da caracterização do crime de **calúnia**, que diz respeito a conduta da pessoa que imputa, falsamente, fato tipificado e penalizado como crime a outrem.

Da mesma forma há reprimenda legal para conduta da pessoa que denegrir a imagem ou reputação de outra pessoa, divulgando algum fato ofensivo, assim estaremos diante do delito de **difamação**.

Agora, quem ofende o decoro de outrem, incitando atributos ou qualidades negativas, defeitos, poderá responder pelo crime de **injúria**.

Caso tenha sido vítima, o que fazer:

a) Se a conversa ocorreu em rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
b) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**
c) O Código Civil assegura a reparação dos danos morais e físicos sofridos e oriundos de ato ilícito, portanto, procurar um advogado para ingressar com ação civil pertinente.

7. “Ransonware” (sequestro de dados)

O golpe ocorre da seguinte forma:

O ransomware é um vírus que “tranca” os seus dados até o pagamento de um resgate.

Na maioria das vezes a invasão ocorre no período da noite ou madrugada, momento em que um criminoso virtual invade o dispositivo da vítima e instala um software capaz de criptografar (codificar) as informações de seu computador. Ao acessar o computador após tal procedimento, a vítima receberá uma mensagem de que seus dados foram criptografados e se ela não realizar um pagamento exigido pelo criminoso, normalmente em bitcoins, a vítima perderá todos os dados do computador invadido.

Como evitar o golpe:

a) Mantenha *backup* atualizado do computador, de preferência em HD externo ou *pen drive* e nunca os deixe espetados no computador, pois também poderão ser invadidos ou infectados;
b) Mantenha antivírus e *firewalls* sempre ativados e atualizados;
c) Evite acesso a sites suspeitos;
d) Não clique em *links* duvidosos de *e-mails* suspeitos.

Caso tenha sido vítima, o que fazer:

a) Não apague os *e-mails* e/ou mensagens recebidas do criminoso;
b) Se houver conversa com o criminoso via rede social, salve o nome do perfil e o *link* completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias, inclusive carteiras eletrônicas de bitcoins informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

8. Golpe do amor / Golpe *Don Juan* / Golpe sentimental

O golpe ocorre da seguinte forma:

Pessoas que estão em busca de um relacionamento amoroso, utilizam plataformas digitais para encontrar o par perfeito. Desta forma, criminosos criam perfis falsos nesses *sites* de relacionamento e, a princípio, por meio de conversas sedutoras e juras de amor, tentam ganhar a confiança da vítima.

Em um segundo momento, após envolver a vítima com declarações de amor, o golpista cria inverdades com intuito de obter vantagem econômica, em prejuízo da vítima.

As mentiras utilizadas pelos criminosos são as mais diversas como, por exemplo, usar a desculpa de que deseja conhecer pessoalmente a vítima e então pedir dinheiro emprestado a ela para comprar supostas passagens; ou então o estelionatário diz que está enviando um presente (jóia, ouro, dólares), mas que para retirar o pacote será necessário pagar uma taxa, fornecendo então uma conta bancária de pessoas de confiança do próprio golpista.

Como evitar o golpe:

a) Procure marcar encontros **pessoais** com o namorado(a) e, preferencialmente, em **locais públicos**;
b) Desconfie da solicitação de empréstimo de altos valores, independentemente da situação relatada;
c) Dialogue com parentes e amigos sobre o seu relacionamento e peça opinião deles sobre qualquer pedido de valor;

Caso tenha sido vítima, o que fazer:

a) Não apague nenhuma da conversas realizadas com o possível criminoso;
b) Tire cópia de todas estas conversas e comprovantes de depósitos ou transferências bancárias realizadas;
c) Anote os dados das contas bancárias para as quais o dinheiro foi enviado, entre em contato com o gerente de sua conta bancária e tente bloquear o valor.
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**

9. Sextorsão

O que é?

É a ameaça de se divulgar imagens ou vídeos íntimos para forçar alguém a fazer algo, seja por vingança, humilhação ou para obter vantagem financeira. É uma forma de violência grave que pode levar a consequências extremas como o suicídio da vítima.

O golpe ocorre da seguinte forma:

As vítimas podem compartilhar uma imagem por um impulso, podem ter tido um relacionamento com o agressor, ou apenas acreditam que ele já tenha alguma imagem íntima delas porque ele insiste que tem; há casos de adolescentes que acreditam estarem conversando com outros adolescentes e enviam fotos íntimas, mas na verdade estão conversando com um criminoso; A obtenção de imagens ou vídeos íntimos também pode acontecer após invasão de contas e/ou dispositivos (hack) ou mediante falsas ofertas de emprego em agências de modelos, em que se pedem fotos e vídeos íntimos. Após obtenção do conteúdo íntimo, as vítimas são ameaçadas para enviarem mais fotos/vídeos, para participarem de um encontro sexual real ao vivo ou para pagarem determinada quantia em dinheiro, tudo em troca de não terem suas imagens íntimas expostas.

Como evitar o golpe:

a) Evite compartilhar fotos e vídeos íntimos;
b) Evite manter fotos e vídeos íntimos em seu celular – caso ele seja roubado o criminoso poderá ter acesso a esse conteúdo;
c) Desconfie de pedidos de amizade vindos de desconhecidos;
d) Evite participar de chamadas de vídeo com desconhecidos e lembre-se que a imagem da pessoa que você está vendo pode ser falsa!
e) Tenha sempre antivírus instalado em seu terminal.

Caso tenha sido vítima, o que fazer:

a) Não apague as conversas mantidas com o criminoso;
b) Se a conversa ocorreu em rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima e sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**

10. Golpes envolvendo PIX

As recomendações com relação às transações PIX são, em geral, as mesmas para proteger o acesso a serviços financeiros já utilizados, como TED e DOC.

Não entre em sites ou instale no celular aplicativos desconhecidos;

Não há sites ou aplicativos do Banco Central ou do Pix criados exclusivamente para cadastramento das chaves, nem para a realização das transações Pix;

O cadastramento das chaves é realizado em ambiente logado no aplicativo ou site da sua instituição de relacionamento, o mesmo que já é utilizado para as demais transações financeiras, como consultar saldo, fazer transferências ou tomar dinheiro emprestado;

O cadastramento das chaves requer o consentimento do cliente e para cadastrar a chave Pix é feita uma validação em duas etapas. O cadastro do número de celular ou do e-mail como chave Pix depende da confirmação por meio de um código que será enviado, por exemplo, por SMS ou para o e-mail informado.

Já o CPF/CNPJ só pode ser usado como chave se estiver vinculado à conta, informação necessária no momento de sua abertura, comprovada por meio de documento.

Se o usuário tem dúvidas, procure se informar através do site da sua instituição de relacionamento.

Não há prazo para o cadastramento das chaves, começou em 05/10 e estará sempre disponível.

Caso tenha sido vítima, o que fazer:

1) Reunir toda documentação da transação (extratos, comprovantes, etc)

2) Registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES** ou registre os fatos presencialmente no Distrito Policial mais próximo da residência.

3) Cientificar o prestador de serviço de pagamento para eventual ressarcimento, após análise dos documentos.